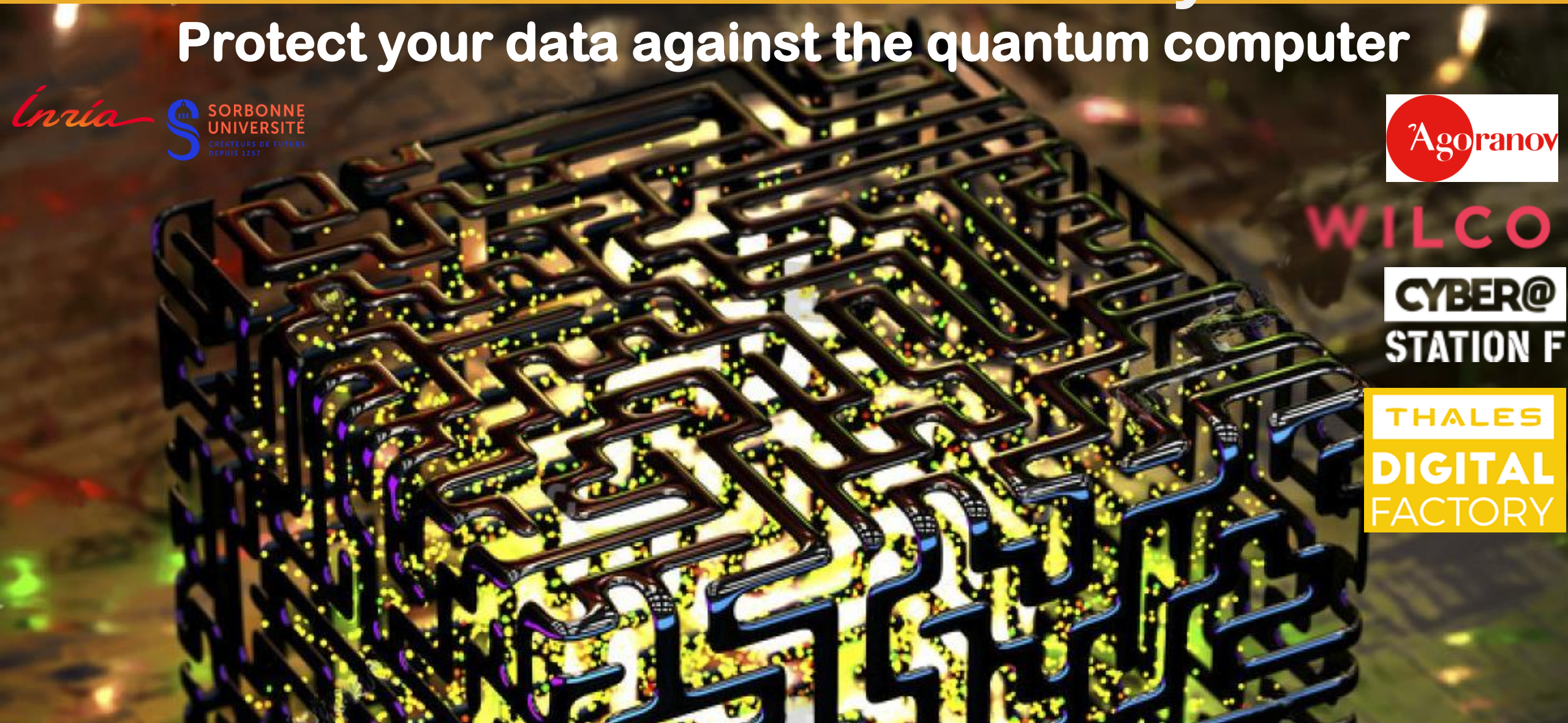
CRYPTONEXT SECURITY

CRYPTONEXT Security

Protect your data against the quantum computer



Inria

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

Agoranov

WILCO

CYBER@ STATION F

THALES DIGITAL FACTORY

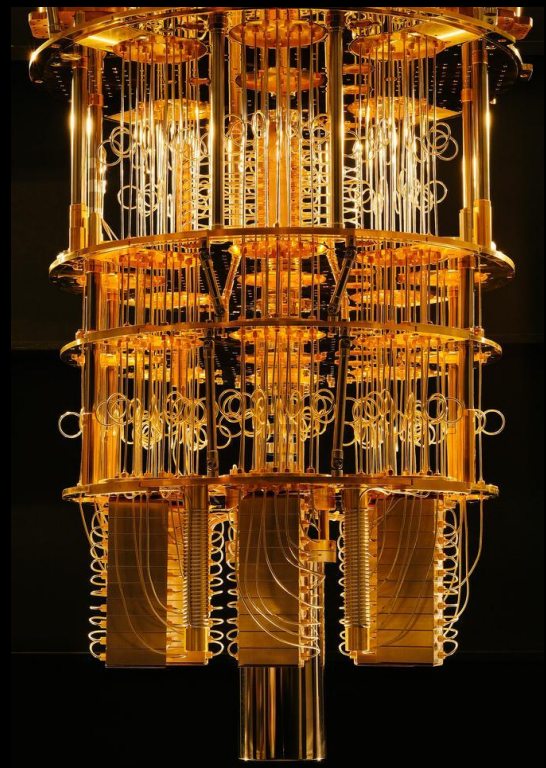
Table des Matières

Menace quantique

Comment maintenir la sécurité numérique ?

CryptoNext Security
Démonstration

Cas d’usages : Blockchain/VPN



L'ORDINATEUR QUANTIQUE : UNE MENACE POUR LA SÉCURITÉ NUMÉRIQUE

L'ordinateur quantique remet complétement en cause la sécurité digitale. Sa puissance permet de casser les standards de cryptographie actuels.

MACHINE	Temps pour casser le standard actuel (RSA-1024)
Classique	~ 400 ans
Quantique	**< 80 minutes**

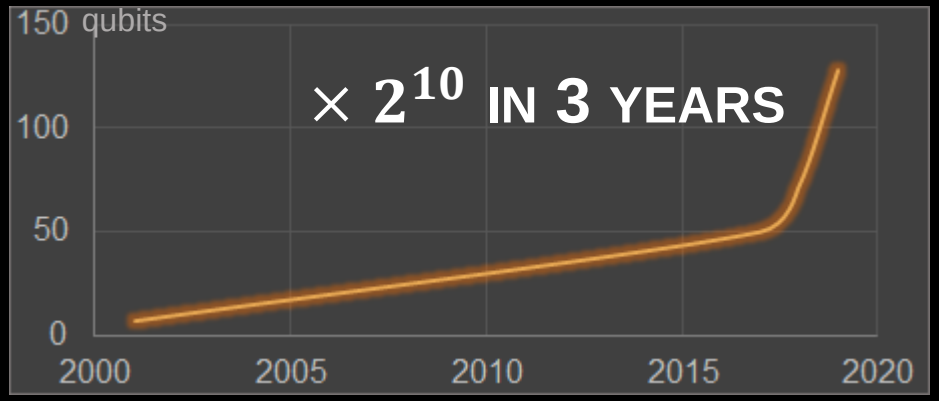
L'ORDINATEUR QUANTIQUE : UNE MENACE POUR LA SÉCURITÉ NUMÉRIQUE

En "vente libre"

ATOS QLM (2017)

IBM Q System One (2019)

Puissance de l'ordinateur quantique



http://www.qubitcounter.com/

RISQUE PERÇU COMME MAJEUR DEPUIS 2016

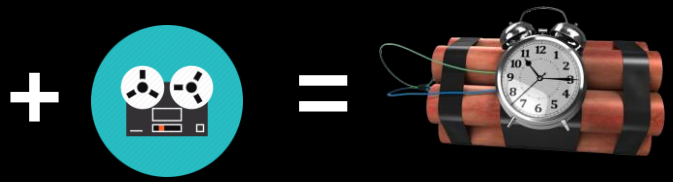
“Quantum risk is now simply too high and can no longer be ignored”.
D. Moody, NIST, 2016.

‘’ Waiting until the last minute to start planning the transition to quantum-safe algorithms unnecessarily puts your organization’s data at risk. Taking these steps will help get your organization ready for the coming transition.’’, DigiCert, 2019.

“My customers are already asking about my transition plan to a quantum-safe cryptography.”
M. Campagna, Amazon Web Service, 2017.

UNE BOMBE À RETARDEMENT SUR LA SÉCURITÉ

On peut dès maintenant enregistrer les données et les déchiffrer plus tard; dès qu'un ordinateur quantique assez puissant sera disponible.

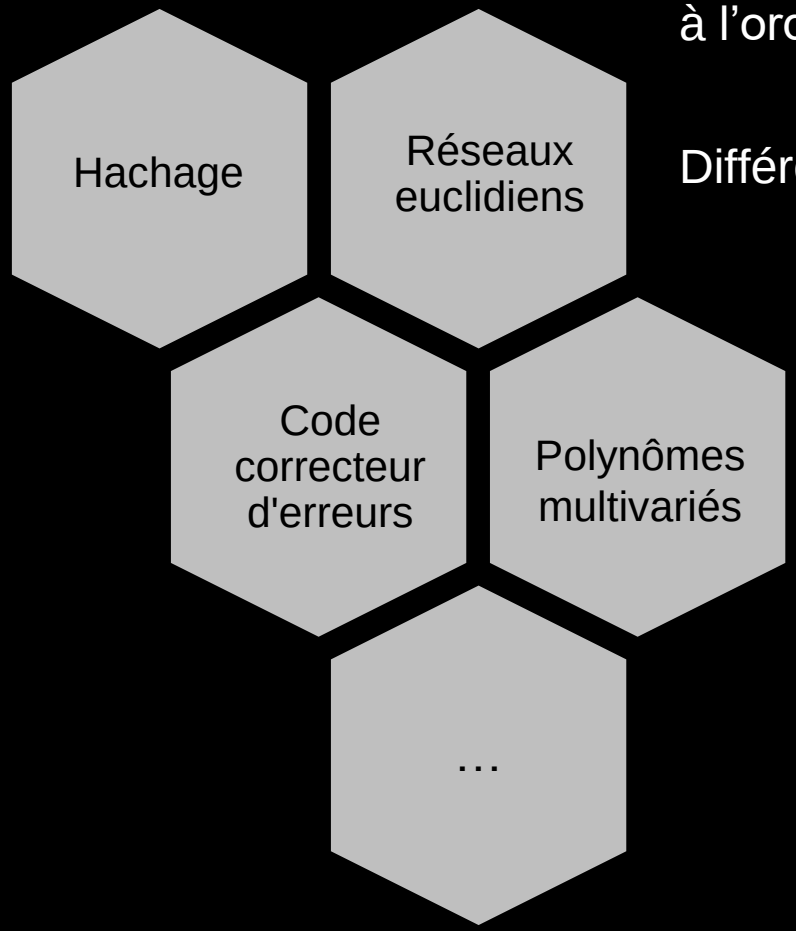


Mais aussi:

Kazakhstan government is now intercepting all HTTPS traffic

COMMENT MAINTENIR LA SÉCURITÉ NUMÉRIQUE ?

La cryptographie au cœur de l'enjeu



Il est nécessaire d'exploiter de nouveaux problèmes mathématiques résistants à l'ordinateur quantique pour imposer de nouveaux standards.

Différentes méthodes mathématiques sont en lice pour la standardisation

Exemple: résoudre des **équations non linéaires**:

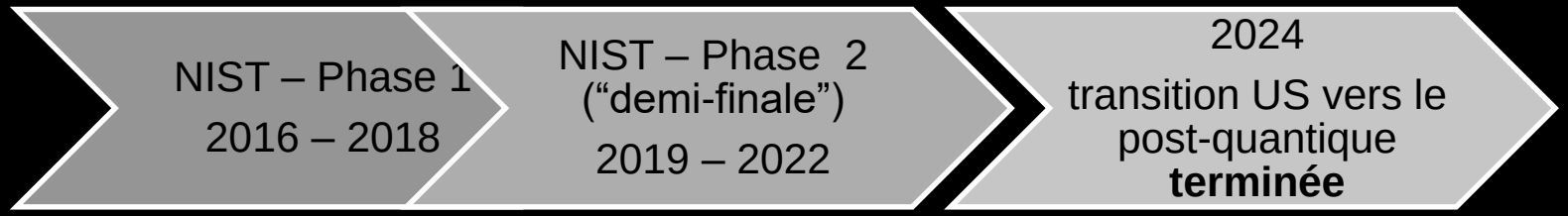
$$\begin{cases} x_1x_4 + x_1x_5 + x_2x_3 + x_2x_4 + x_3x_4 + x_4 + x_5 + 1 = 0 \\ x_1x_3 + x_1x_5 + x_2x_4 + x_3x_4 + x_3x_5 + x_2 + x_5 + 1 = 0 \\ x_1x_3 + x_1x_4 + x_1x_5 + x_2x_5 + x_3 + x_4 = 0 \\ x_1x_3 + x_1x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_5 + x_4x_5 + x_1 + x_5 + 1 = 0 \\ x_1x_2 + x_1x_4 + x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4 + x_4x_5 + x_1 = 0 \end{cases}$$

NOUVEAUX STANDARDS RÉSISTANTS À L'ORDINATEUR QUANTIQUE

- NIST : nouveaux standards cryptographiques en cours de préparation

> *" …. transition of US IT government infrastructure to a post-quantum cryptography will be completed by **2024**".*
> M. Scholl, NIST, 2017.

National Institute of Standards and Technology



STANDARDS PROTOCOLAIRES

- De nouveaux standards à venir pour chaque cas d'utilisation
- International : ISO ITU (X509)
- Internet : IETF (TLS)
- Finance : ASC X9, Pôle Finance Innovation
- Européen : ETSI (VPN)
- Chinois : processus concurrent

POSITION FRANÇAISE

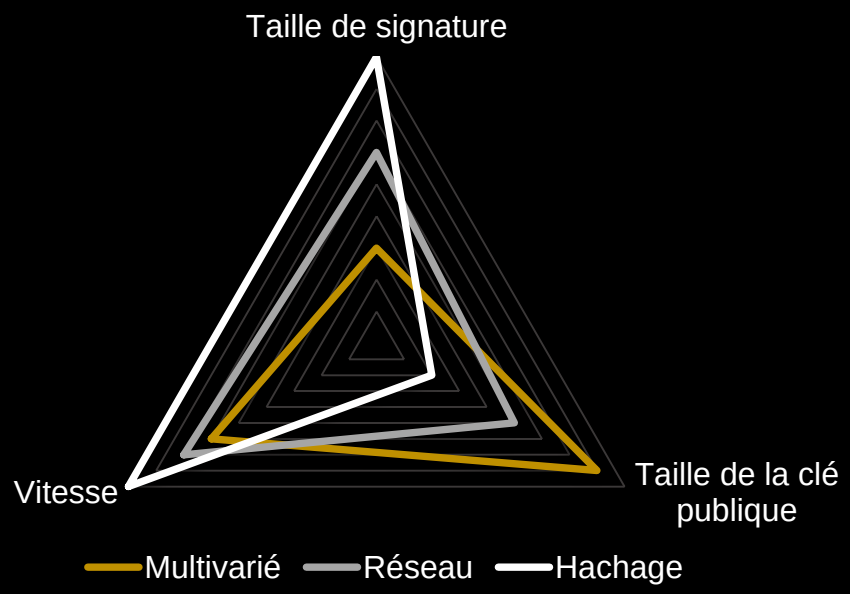
- ANSSI : pousse pour une adoption rapide de solutions hybrides combinant sécurité classique & post-quantique

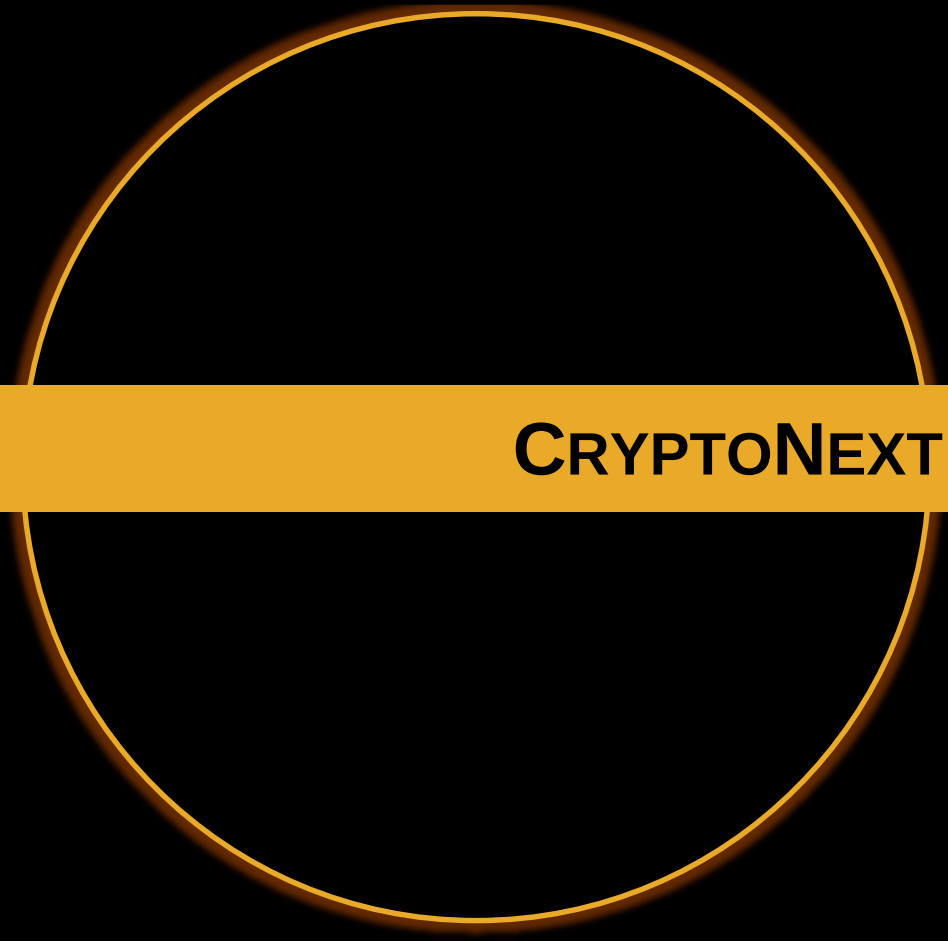
> *"For use cases requiring a long-lived protection of the information (≥ 20 years), it is advised to start taking the quantum threat into account",*
> *H. Gilbert, ANSSI, 2018.*

> *"L'ANSSI a commencé à travailler sur ces questions, en annonçant par exemple qu'à compter de 2020, elle ne labelliserait plus les technologies de chiffrement qui ne résisteraient pas au quantique",*
> *P. Forteza, Députée en charge du quantique , Monde Informatique 2019.*

Plusieurs solutions en fonction des usages

- Chaque méthode en lice pour la standardisation possède ses avantages et ses inconvénients en fonction des domaines d'application.
- Plusieurs algorithmes cryptographiques seront retenus.
- L'optimisation est la clé du déploiement de ces nouveaux protocoles.
- Elle nécessite une très bonne connaissance des différentes briques mathématiques.



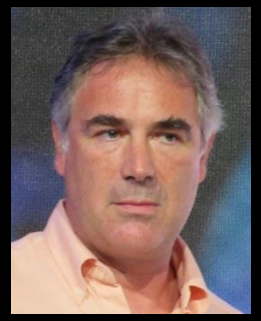


CryptoNext Security

CryptoNext Security

- CryptoNext Security, leader scientifique mondial, plus de 20 ans de savoir faire post-quantique issu de Inria/Sorbonne Université
- L'expertise de CryptoNext repose sur plus de 150 publications sur
  - Conception d'algorithmes post-quantiques (sélectionné pour la demi-finale du processus NIST)
  - Cryptanalyse (cassage) des algorithmes existants
- Une implication très forte dans les activités de standardisation NIST, ETSI, une expertise sur toutes les fonctions en cours de standardisation
- Une technologie hybride, facilement intégrable dans un produit de sécurité et transparente pour l'utilisateur final, déployée et testée depuis 2016

CRYPTONEXT SECURITY



Jean-Charles Faugère, CTO,
PhD, HDR, DR INRIA, Chef d'équipe
Cray & Atos Prizes
150 publications scientifiques

Ludovic Perret, CEO,
PhD, HDR

Atos prize
Standardisation
60 publications

Frédéric de Portzamparc, COO,
X07, PhD,

Formerly Strategic Marketing with tech start-up,
Senior Security Consultant at Thales (Gemalto)

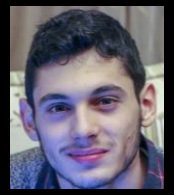
CRYPTONEXT SECURITY

R. P. Straub
Business stratégie
Ancien VP sales (ID Quantique)

Apporteurs d'affaires

A. Chance
Investor (BA) + Business developper

P.De Perthuis
(Centrale)



S. Rastikian
(ENS)

O. Breysse

We work together with

QUANTONATION
Capital Investors for the Quantum Future

NDA-Security
Ressources Conseil Expertise Projets SSI

C.-H. Mathorel

Advisory Board

P. Duluc
CTO Big Data & Security
ATOS

B. LaMacchia
Responsable Sécurité et cryptographie
Microsoft

D. Mercier (ancien commandement suprême transformation de l'OTAN, DG adjoint de Fives Group)

R. Marino
Fondateur DeepTech Founders

D. Stehlé
Professeur ENS Lyon
ERC, médaille de bronze CNRS

Ce que propose CryptoNext Security

Des algorithmes ultra-optimisées pour des besoins et contraintes spécifiques

- Latence, débit, empreinte mémoire, taille de clés

Des solutions post-quantiques clé-en-main de protocoles sécurisés

- Canal sécurisé par VPN
- PKI
- Blockchain

Du conseil fondé sur une expertise unique

- Analyse d'impact du risque quantique
- Elaboration de solutions optimales (coût/performance)

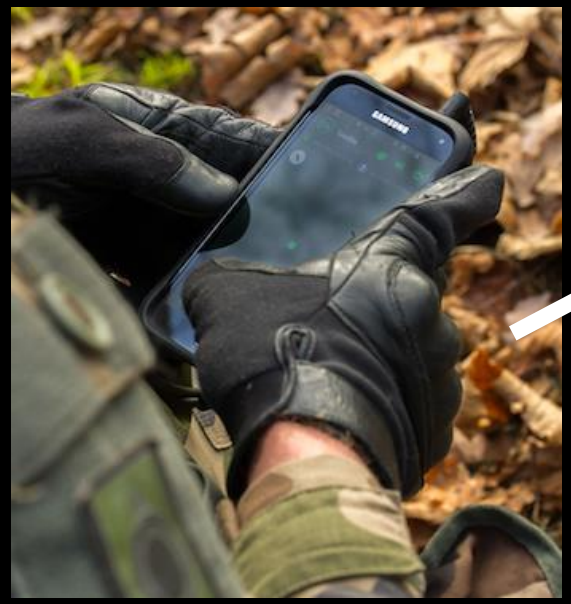
DÉMONSTRATION D'UNE TECHNOLOGIE CRYPTONEXT SECURITY

EXEMPLE DE TECHNOLOGIE MATURÉE ET TESTÉE DEPUIS 2016

Prototypage et validation terrain avec l'Armée de Terre d'une messagerie sécurisée contre les ordinateurs quantiques.

Photos issues du test terrain Base de Saint-Germain-en-Laye (150 participants)

DÉMONSTRATION



Utilisateur 3

Message

Utilisateur 1

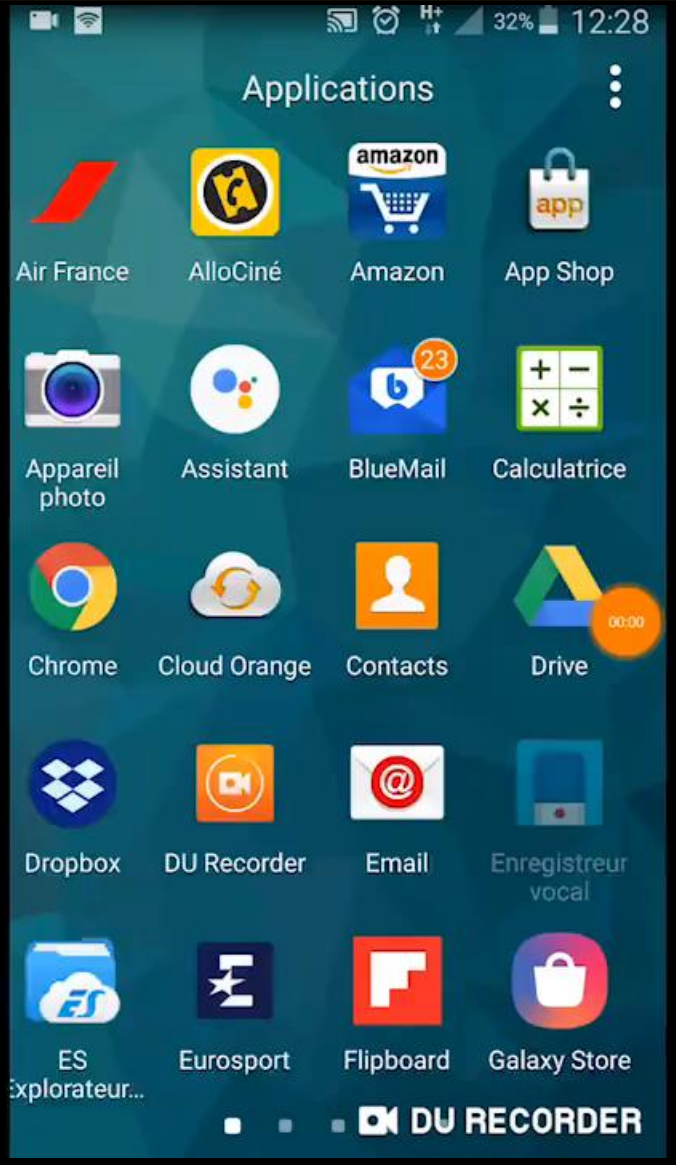
Message

Document

Utilisateur 2

Echange de clé post-quantique
+ AES

DÉMONSTRATION

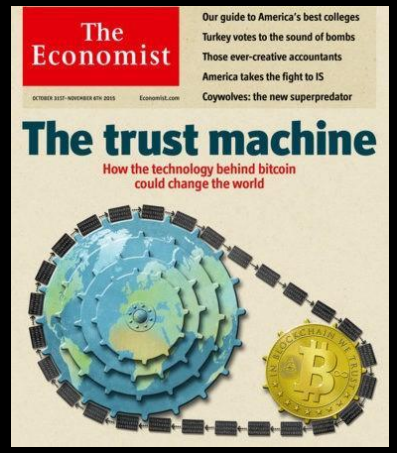


FOCUS : IMPACT SUR LA BLOCKCHAIN

LA BLOCKCHAIN MENACÉE PAR L'ORDINATEUR QUANTIQUE

Notariser, horodater, tracer des informations sur un registre distribué infalsifiable et immuable, telles sont les promesses de la technologie blockchain.

2015 → **2025**



?

TRUST

L'ordinateur quantique remet en cause la sécurité des blockchains et donc la confiance dans leur pérennité.

IMPACT SUR LA BLOCKCHAIN

Cryptographie à clé secrète

Fonction de hachage

Inverser la fonction (k est la taille de la sortie)

Classique	$O(2^k)$	Recherche exhaustive
Quantique	$O(2^{\frac{k}{2}})$	Algorithme de Grover

Cryptographie à clé publique

Signature numérique

clé secrète : signer la transaction

clé publique : verifier la validité d'une signature

Retrouver la clé secrète (RSA-1024)

Classique	~ 400 ans
Quantique	**< 1h**

ANALYSE DU CAS BITCOIN

Fonction de hachage

"We find that the proof-of-work used by Bitcoin is relatively resistant to substantial speedup by quantum computers in the next 10 years."

Signature numérique

"On the other hand, the elliptic curve signature scheme used by Bitcoin is much more at risk, and could be completely broken by a quantum computer as early as 2027."

"*Quantum attacks on Bitcoin, and how to protect against them*", D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, M. Tomamichel, 2017.

BLOCKCHAIN RÉSISTANTE AU QUANTIQUE (1/4)

Blockchain du marché

Résistance au quantique

- Sécurité à long terme
- Intégration simple
- Pérennité de la solution

Exemple de réalisation CryptoNext:

Intégration dans CORDA (consortium de banques R3)

Version post-quantique de CORDA

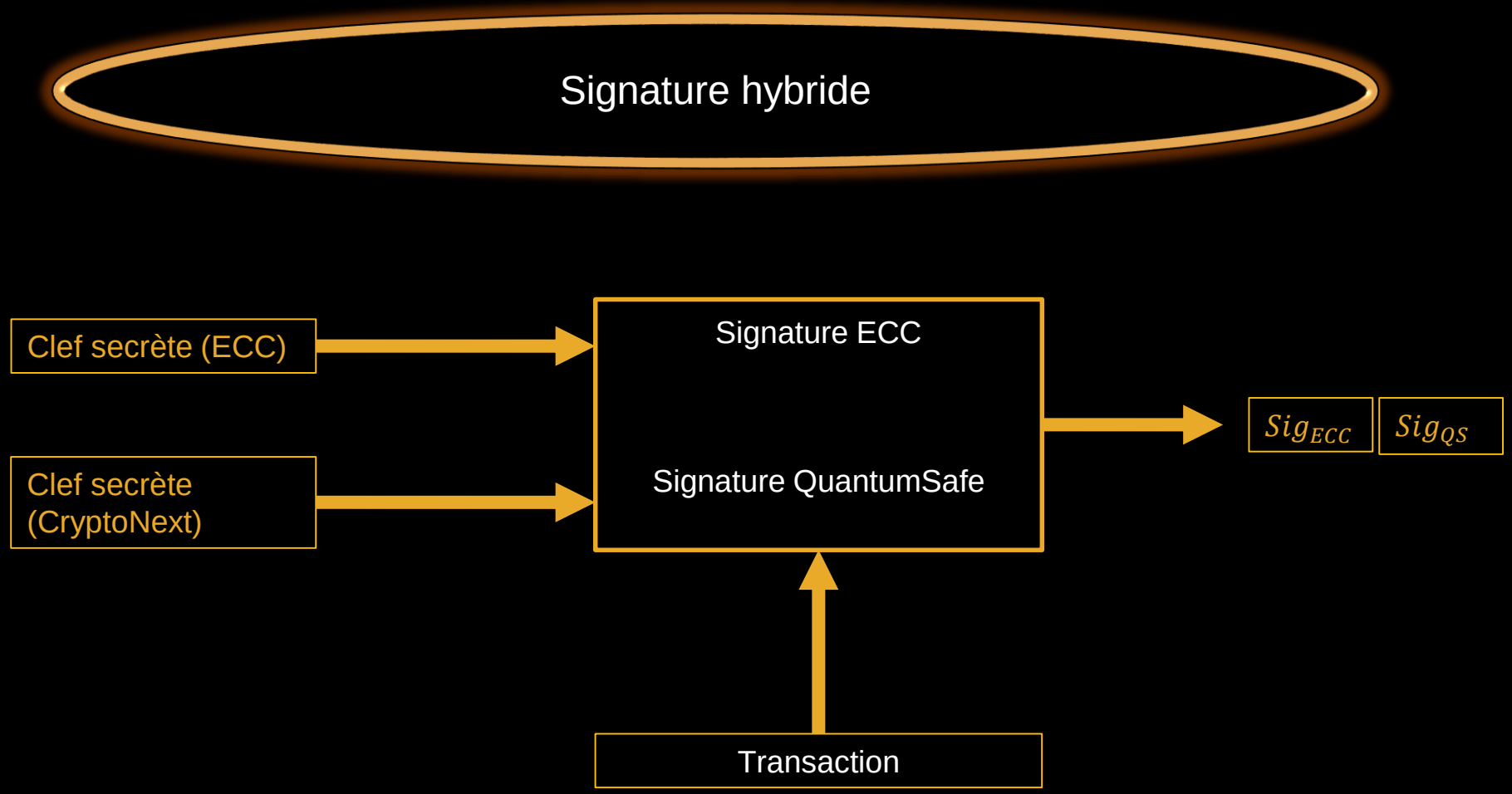
HyberLedger en cours

BLOCKCHAIN RÉSISTANTE AU QUANTIQUE (2/4)

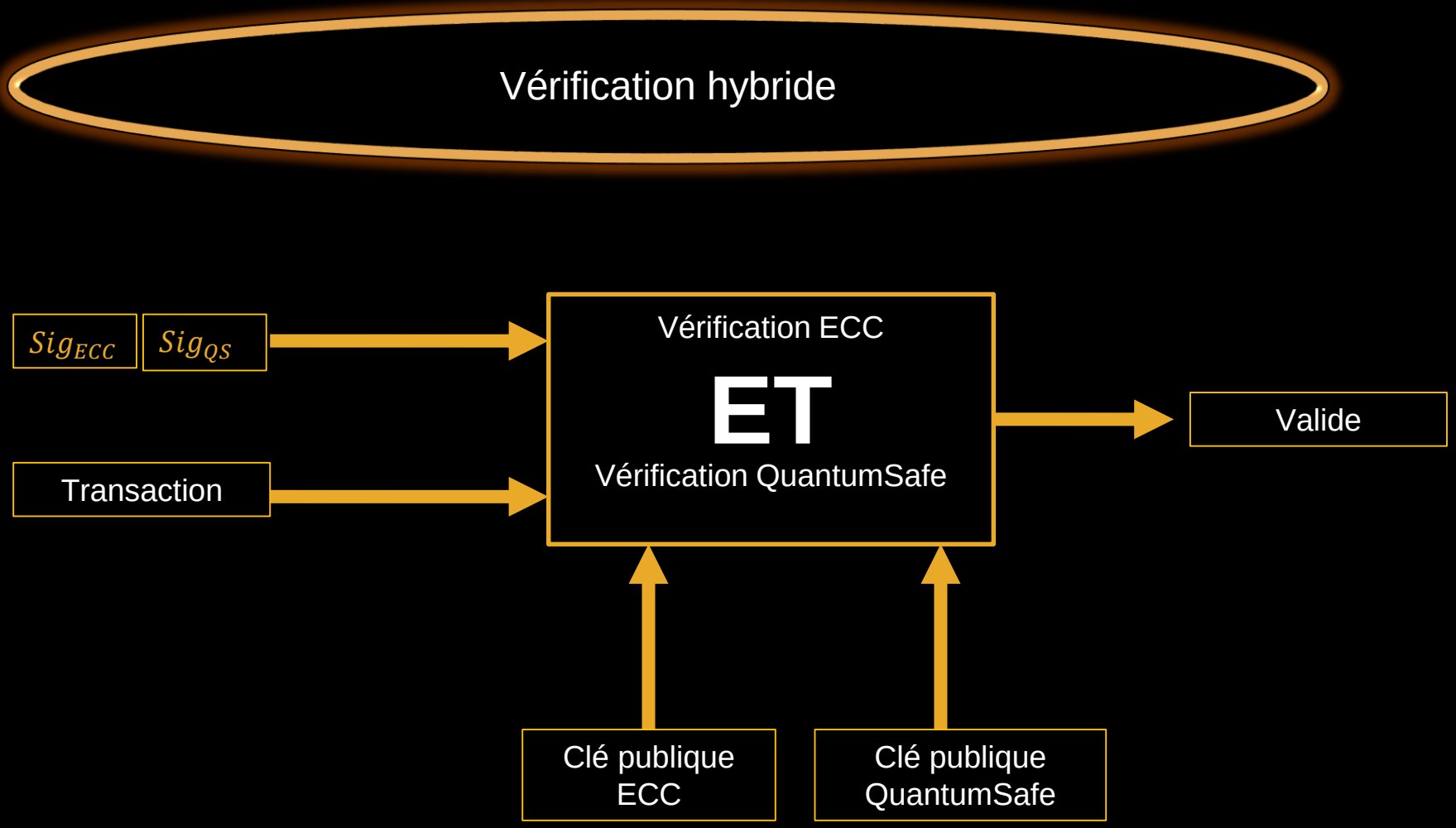
How do I prove a Blockchain transaction is mine ?

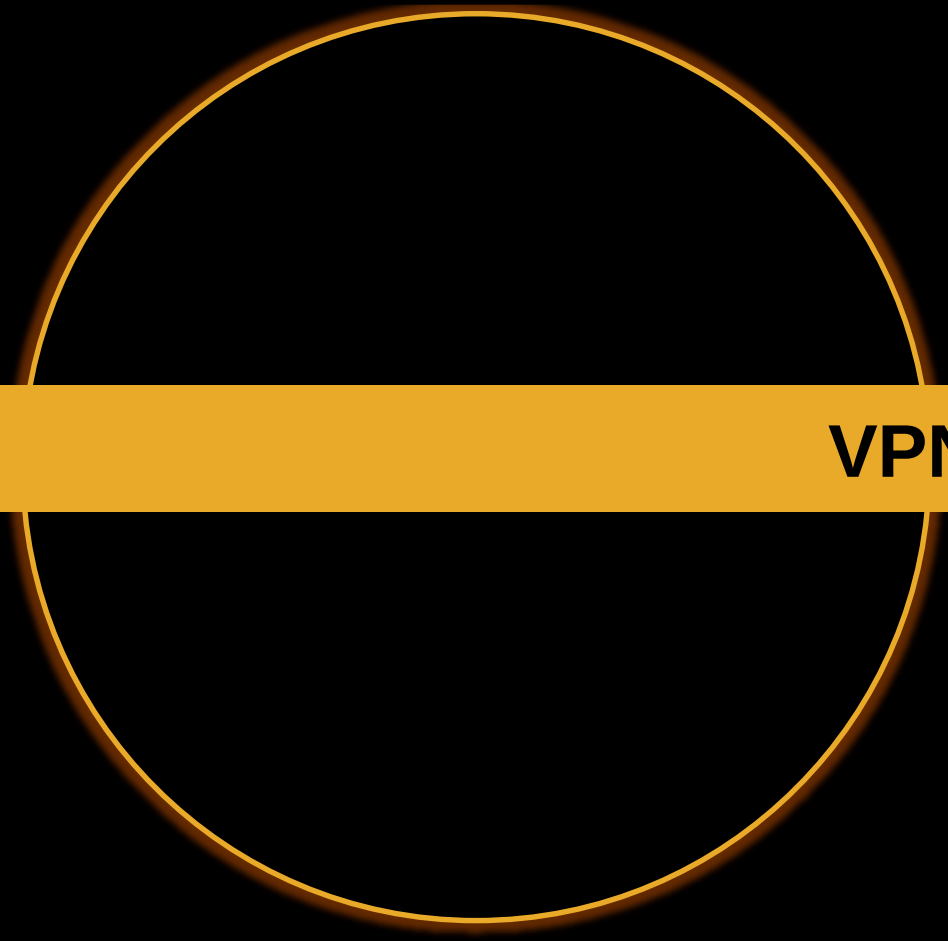
1. Create Private- and the matching Public-key,
2. Use the Public-key as seed text to create a new hash-address,
3. Sign the new hash-address with your private-key
4. Validate the Signature/ Hash-address combination with the public-key.

BLOCKCHAIN RÉSISTANTE AU QUANTIQUE (3/4)



BLOCKCHAIN RÉSISTANTE AU QUANTIQUE (4/4)





VPN

VPN RÉSISTANT AU QUANTIQUE

- Sécurité à long terme
- Intégration simple
- Pérennité de la solution

Solution quantum-safe

CONTACTEZ-NOUS !

ludovic.perret@cryptonext-security.com
Frederic.de.Portzamparc@cryptonext-security.com
jcf@cryptonext-security.com

www.cryptonext-security.com